Audit Report

YEAR 2000 CONVERSION WITHIN THE
DEFENSE SECURITY SERVICE

Report No. 99-185 June 11, 1999

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD, Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DCII	Defense Clearance and Investigations Index
DSS	Defense Security Service
FASS	Files Automation and Scanning Subsystem

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

June 11, 1999

MEMORANDUM FOR DIRECTOR, DEFENSE SECURITY SERVICE

SUBJECT: Audit Report on Year 2000 Conversion Within the Defense Security Service (Report No. 99-185)

We are providing this final report for your information and use. We considered management comments on a draft of this report when preparing the final report.

The Defense Security Service comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Robert K. West at (703) 604-8983 (DSN 664-8983) (email rwest@dodig.osd.mil) or Mrs. Yvonne M. Speight at (703) 604-8990 (DSN 664-8990) (email yspeight@dodig.osd.mil). See Appendix C for the report distribution. A list of the audit team members is on the inside back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-185 **June 11, 1999**
(Project No. 9AD-0084)

Year 2000 Conversion Within the Defense Security Service

Executive Summary

Introduction. This report is one in a series issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor efforts to address the year 2000 computing challenge. For a listing of audit projects addressing the issue, see the year 2000 webpage on the Inspector General Internet at http://www.ignet.gov.

Objectives. Our objective was to determine whether the Defense Security Service effectively planned, executed, and coordinated year 2000 management strategies to ensure that year 2000 related issues would not unduly disrupt operations. Specifically, we reviewed actions that the Defense Security Service took to identify systems; assess risk; prepare system contingency plans, operational contingency plans, and test plans; and address other critical areas that could adversely affect its mission.

Audit Results. The Defense Security Service was behind the prescribed DoD schedule for year 2000 conversion and needed to accelerate its effort. During the audit, management took action to address deficiencies in system status, reporting, and interface agreements. Additional areas of concern included:

- The Defense Security Service did not prepare system or operational contingency plans. As a result, the Defense Security Service must do more to minimize the risk of mission disruption in the year 2000 (Finding A).

- The Defense Security Service test plan did not provide sufficient detail to adequately test 15 mission-essential systems for year 2000 compliance, and the milestone dates for system tests and end-to-end testing were unrealistic. In addition, the Defense Security Service did not prepare an end-to-end test plan to make an operational readiness assessment of its personnel security investigative and industrial security programs. As a result, there is continued risk that the Defense Security Service mission-essential systems may have year 2000 related failures, and the failures could result in the Defense Security Service not accomplishing its mission effectively (Finding B).

Summary of Recommendations. We recommend that the Defense Security Service prepare system contingency plans for each mission-essential system and prepare operational contingency plans for each site location and the field security investigative function. The operational contingency plans should address power and communication

services. We also recommend that the Defense Security Service use the DoD Year 2000 Management Plan as a framework to revise its test plan to address year 2000 compliance testing required for each mission-essential system and prepare an end-to-end test plan. We also recommend that the Defense Security Service revise its test schedule to reflect new milestone dates for system and end-to-end testing, complete the retesting of systems previously tested but lacking formal documentation and certification, test the remaining mission-essential systems, document test results for all systems, and certify all systems as year 2000 compliant upon successful completion of the tests. We also recommend that the Defense Security Service provide an end-to-end test plan to the Year 2000 Office for review.

Management Comments. The Director, Defense Security Service, concurred with the findings and recommendations in this report and stated that his agency had made significant progress in its year 2000 conversion effort. The corrective actions taken and planned by management are responsive. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Table of Contents

Background

Year 2000 Problem. This report is one in a series issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor efforts to address the year 2000 computing challenge. Because of the potential failure of computers to run or function throughout the Government, the President issued Executive Order 13073, "Year 2000 Conversion," February 4, 1998. The Executive Order directs Federal agencies to ensure that no critical Federal program experiences disruption because of the year 2000 problem and ensure that efforts to address the year 2000 problem receive the highest priority attention.

DoD Year 2000 Management Strategy. The "DoD Year 2000 Management Plan" (the DoD Year 2000 Plan) describes a five-phase year 2000 management process, which consists of awareness, assessment, renovation, validation, and implementation phases. Although the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued draft versions of the DoD Year 2000 Plan, DoD intended Defense Components to accomplish the phases within the target dates shown in the document. The final version established December 31, 1998, as the target date for deploying renovated mission-critical systems and completing contingency plans for those systems. The DoD Year 2000 Plan established March 31, 1999, as the target date for deploying renovated mission-essential systems, completing contingency plans for those systems, and completing operational contingency plans. By June 30, 1999, the DoD Year 2000 Plan requires DoD Components to exercise all plans to assure their viability.

Defense Security Service Missions. On November 25, 1997, the DoD Reform Initiative Directive No. 2 renamed the Defense Investigative Service to the Defense Security Service (DSS). Directive No. 2 also implemented the integration of the DoD Security Institute; the Security Research Center, formally the Personnel Security Research Center, Monterey, California; and the DoD Polygraph Institute, Fort McClellan, Alabama. The DoD Security Institute functions were transferred to the DSS Training Office. The DoD Polygraph Institute remains autonomous and reports directly to the Director, DSS. The reorganization of DSS established three missions within the organization. Those missions are personnel security investigations, industrial security, and security education and training. The DSS sites include the headquarters in Alexandria, Virginia; two operations centers located in Linthicum, Maryland, and Columbus, Ohio; and 13 operating locations with 1,150 special agents and 208 industrial security representatives in remote locations. The Office of the Secretary of Defense principal staff assistant for DSS is the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence).

Objectives

The audit objective was to determine whether DSS effectively planned, executed, and coordinated year 2000 management strategies to ensure that year 2000 related issues would not unduly disrupt operations. Specifically, the audit addressed the actions taken by DSS to identify systems; assess risk; prepare system contingency plans, operational contingency plans, and test plans; and address other critical areas that would adversely affect its mission. See Appendix A for a discussion of the audit scope and methodology.

Reclassification of Defense Security Service Systems

The DoD Year 2000 Plan, December 1998, states that mission-critical systems include those required to perform Department-level and DoD Component-level core functions. The DoD Year 2000 Plan defines mission-essential systems as systems the loss of which would have an adverse impact upon the overall organization's mission functionality and, if not corrected, of which degradation would cause loss of mission capability. The Director, DSS, considers a DSS system mission-critical if it is needed to support the investigative mission or to manage organizational administrative functions.

Before the start of the audit, DSS categorized and reported 21 systems as mission-critical, reported 1 system as mission-essential, and had not identified 2 systems. The 21 systems were reported as mission-critical in the DoD year 2000 database but DoD did not report the systems as mission-critical to the Office of Management and Budget. We brought the discrepancy in reporting to the attention of DSS year 2000 management personnel and informed them that DoD would be using the DoD year 2000 database to report the status of mission-critical and mission-essential systems to the Office of Management and Budget for the April 1999 quarterly report. To assure consistency in reporting, DSS officials stated that DSS would report its 24 systems as mission-essential to the DoD database.

External Interface Agreements

After this audit began, DSS began aggressively pursuing external interface agreements. In June 1998, the DSS year 2000 management team discussed interface agreements with program managers. DSS identified 23 external organizations that interfaced with its systems. DSS did not begin finalizing formal interface agreements until after the start of this audit. Initially, DSS believed that formal interface agreements were not necessary for 12 of the 23 external organizations because those organizations were in the intelligence community and were reported in the Intelligence Community External Interface Tracking Systems database. The Intelligence Community Year 2000 Working Group established the database to allow organizations within the intelligence

community to input information on their systems that interface with other intelligence organizations. The March 25, 1998, minutes of the Intelligence Community Year 2000 Working Group state that the database was crucial in maintaining a central repository of information on intelligence systems, identifying matching interfaces between intelligence organizations, and validating the completed coordination of interfacing systems between intelligence organizations. The members of the working group agreed that if the interfacing organizations affirmed matching systems that affirmation would constitute an interface agreement. The requirement to have a signed memorandum of agreement in addition to the database match and coordination was not resolved by all members. Each organization would determine whether a formal interface agreement was necessary. However, in the Intelligence Community Year 2000 Working Group meeting held July 29, 1998, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) required that all DoD intelligence organizations obtain formal interface agreements. As a result, the Intelligence Community Year 2000 External Interface Tracking Systems became a database to document and record interface agreements.

Before the start of the audit, DSS was not aware of the change in the use of the database and, therefore, had not obtained formal agreements with intelligence organizations that interface with its systems. After the audit team informed a representative of the DSS year 2000 management team that formal interface agreements were required for interfacing systems within the intelligence community, DSS took action to obtain the agreements. A formal agreement with the Army Central Personnel Security Clearance Facility was finalized on January 6, 1999.

Of the remaining 11 external interfacing organizations, DSS began requesting formal written agreements in late December 1998. DSS requested one interface agreement on December 23, 1998; nine interface-agreement letters were sent out on February 17 and 18, 1999; and the last letter was sent on February 26, 1999. As of March 26, 1999, four interface agreements had been finalized.

A. Contingency Planning

DSS did not prepare system contingency plans and operational contingency plans. DSS delayed the preparation of system contingency plans because management believed that newly implemented systems were designed year 2000 compliant. Also, DSS believed that the power and communication infrastructure would be fully operational in the year 2000 because they were tenants of other organizations. As a result, DSS must do more to minimize the risk of mission disruption in the year 2000.

DoD Year 2000 Management Plan

The DoD Year 2000 Plan states that a contingency plan identifies steps that would streamline decisionmaking during a year 2000 related failure to enable resumption of mission operations at the earliest possible time, in the most cost-effective manner. The DoD Year 2000 Plan requires DoD Components to develop two types of contingency plans: system and operational.

System Contingency Plans. System contingency plans identify the procedures that system managers would use to restore functionality to a system that could experience a year 2000 related failure. The DoD Year 2000 Plan required development of system contingency plans for mission-critical systems by December 31, 1998, and for mission-essential systems by March 31, 1999, and strongly recommended plans for other systems that have multiple interfaces by March 31, 1999.

Operational Contingency Plans. Operational contingency plans identify procedures that an organization would use to accomplish a mission if a system were disrupted because of a year 2000 computing problem. The year 2000 computing problem could affect the system itself, the power supply, or communication services. Operational contingency plans were due by March 31, 1999.

DSS Contingency Plan Development

DSS did not prepare a system contingency plan for each mission-essential system and did not prepare operational contingency plans. Fifteen[1] of the 24 DSS mission-essential systems being reported will be operational in the year 2000 and beyond. Of the 15 systems, DSS self-certified 8 systems, but could only provide completed checklists for 5 systems. The remaining seven systems were not certified as year 2000 compliant and required additional work.

[1] Appendix B numbers 1 through 15.

DSS Mission-Essential Systems. Of the seven mission-essential systems that were not certified as year 2000 compliant, five[1] systems were not scheduled for year 2000 compliance until after March 31, 1999. The DoD Year 2000 Plan established March 31, 1999, as the target date for fully implementing mission-essential systems. In addition, 4[2] of the 15 systems have multiple external interfaces with other DoD and Federal organizations. Although reported to DoD as mission-essential systems, the Director, DSS, believes that 14 of the 15 systems are critical to DSS in performing its operational missions. DSS had classified the 14 systems as mission critical until February 17, 1999, when it reclassified them as mission essential. (See page 2 of this report for details on the reclassification of the systems.)

DSS prepared a contingency plan for the initial implementation of the Case Control Management System. That plan marginally addressed contingencies for transmitting data to and from external interfaces with the Case Control Management System if the system experienced problems during implementation. After the Case Control Management System became fully operational, the Case Control Management System contingency implementation plan became obsolete. Therefore, DSS still needs to prepare a year 2000-system contingency plan for the Case Control Management System.

Prior to the start of this audit, DSS had not prepared system contingency plans for all of its 15 mission-essential systems as required by the DoD Year 2000 Plan. However, subsequent to the issuance of the draft to this report, DSS has prepared system contingency plans for the Electronic Personnel Security Questionnaire, the FINCEN-Treasury System, the Industrial Security System, the User Community Management System, the Defense Clearance and Investigations Index (DCII), the Student Information and Registration Network, and the Automated Credit Manager. DSS is scheduling workshops to prepare system contingency plans for is remaining eight mission-essential systems.

The Student Information and Registration Network System is a prime example of a system that needed a contingency plan. Before the start of this audit, DSS was not aware that the Student Information and Registration Network 01 within the DSS Training Office was not year 2000 compliant, and DSS had not considered preparing a contingency plan for the system. Because the system is essential to the DSS security-training mission, DSS contracted with a vendor through the General Services Administration to identify a replacement system. The statement of work requires the vendor to evaluate the feasibility of using commercial off-the-shelf products or the Defense Acquisition University system. The statement of work required the vendor to complete the effort by May 1, 1999. The General Services Administration awarded the contract on March 12,

[1] The five systems are the Files Automation and Scanning Subsystem, the Industrial Security System, the Automated Credit Manager, the Field Agent Manager, and the Student Information and Registration Network.

[2] The four systems are the Case Control Management System, the Defense Clearance and Investigations Index, the Automated Credit Manager, and the FINCEN-Treasury System.

1999. DSS has required the contractor to prepare a system contingency plan for the Student Information and Registration Network in case the system failed or was not fully operational by July 1, 1999.

Operational Missions. DSS has the following three operational missions: the personnel security investigations program, the industrial security program, and security education and training. To accomplish the personnel security investigations mission, DSS has 1,150 special agents located across the United States. The special agents transmit data to agency systems located at the Operations Center-Baltimore, Linthicum, Maryland. To accomplish the industrial security mission, DSS has 208 industrial security representatives who review DoD contractor facility operations. To accomplish the security education and training mission, DSS uses the Student Information and Registration Network System to register about 5,000 students for 140 courses annually. In October 1998, DSS brought on-line new systems under its automated data processing modernization program and retired old Defense Investigative Service systems. As a result of the automated modernization program, the disaster recovery plans that were in effect for the former Defense Investigative Service organization and the contingency implementation plan for the Case Control Management System became obsolete. Since October 1996, DSS concentrated its efforts on obtaining, installing, and implementing the new automated systems. Consequently, DSS did not prepare operational contingency plans to address continuity of operations for the DSS Headquarters; the Operations Centers at Linthicum, Maryland, and Columbus, Ohio; the Security Research Center; the DoD Polygraph Institute; the 13 operating locations; and the field security investigative function. Subsequent to the issuance of the draft of this report, DSS prepared a template that will be used by each of its operating sites to develop an operational contingency plan. Each DSS site will forward its completed operational contingency plans to the DSS year 2000 management team and senior management for final review. The DSS goal is to finalize operational contingency plans by September 30, 1999.

As an example, the Security Research Center needed operational contingency plans because of noncompliant software applications. The Security Research Center had numerous software applications that were not year 2000 compliant, that had date-related issues, or for which the status was unknown. The Security Research Center year 2000 management personnel did not begin assessing and testing its hardware infrastructure and software applications until receipt of a December 22, 1998, memorandum from the Director, DSS, tasking all regional activities to test their systems for year 2000 compliance. The Security Research Center year 2000 management personnel identified 7 computer hardware platforms and 120 software applications. Using the Joint Interoperability Test Command year 2000 test tools, Security Research Center personnel determined that the seven hardware platforms were year 2000 compliant. Of 120 software applications, 22 applications were not year 2000 compliant, had date-related issues, or had an unknown status. If operational contingency plans were not prepared, the Security Research Center operations could have been disrupted by year 2000 related software failures. Since the issuance of the draft of this report, DSS management stated that the Security Research Center has completed a thorough year 2000 compliance review of all information technology

components and that those components will be year 2000 compliant by June 30, 1999. Also, the Security Research Center will have a completed operational contingency plan by June 30, 1999.

New Systems Designed for Year 2000 Compliance

DSS delayed preparing system contingency plans because DSS believed that the newly implemented systems for its automated data processing modernization program were designed for year 2000 compliance. Also, DSS did not consider operational contingency plans to address power and communication services because DSS organizational units are tenants of other organizations.

New Systems. In 1996, DSS initiated the automated data processing modernization program to improve the way that it does business in all functional areas. To execute the modernization program, DSS contracted for new automated systems. DSS believed that the new systems would be designed year 2000 compliant and that they had a low risk for year 2000 related failure. Therefore, DSS did not make contingency planning a high priority. However, the contracts for the design of the new systems did not include year 2000 clauses when they were awarded. As a consequence, DSS had no assurance that the new systems were designed year 2000 compliant. DSS must prepare system contingency plans for each of its mission-essential systems.

Power. As tenants in General Services Administration leased buildings and on military installations, DSS believed that the facility owner would have contingency plans for power outages. DSS year 2000 management personnel initiated an effort to review the General Services Administration and military installation web sites to determine the contingency plans for each facility. DSS must prepare operational contingency plans that supplement the plans of facility owners. In addition, DSS has many remote locations, such as field investigators' homes that could experience year 2000 related power outages. DSS must prepare contingency plans that address how field investigators would continue operations if power outages occur at their homes or remote locations.

Communications. The Defense Information Systems Agency maintains DSS communication services. DSS believed that the Defense Information Systems Agency would ensure that all communication systems would be year 2000 compliant. After this audit began, DSS began communicating with the Defense Information Systems Agency and determining what the agency had done to test for year 2000 compliance and what its continuity-of-operation plans were. For the DSS Operations Center, Linthicum, Maryland, DSS has a dial-in backup system that allows calls to be routed through another server if the main server is down. In addition to the dial-in backup system, DSS needs to consider work-around strategies if telephonic communication services should fail. DSS needs to prepare contingency plans that address loss of telephonic communication systems.

Mission Performance in the Year 2000

If mission-essential systems cannot operate because of year 2000 related failure and viable contingency plans are not in place, DSS may not be able to perform its mission effectively. The implementation of the following recommendations should reduce the likelihood of mission disruptions from year 2000 system related failures.

Recommendations and Management Comments

A. We recommend that the Director, Defense Security Service:

1. Prepare system contingency plans for the 15 Defense Security Service mission-essential systems lacking such plans.

2. Prepare operational contingency plans for the Defense Security Service Headquarters; the Operations Centers at Linthicum, Maryland, and Columbus, Ohio; the Security Research Center; the DoD Polygraph Institute; the 13 operating locations; and the field security investigative function. The operational contingency plans should address power outages and communication services. The Defense Security Service should develop all plans in accordance with the DoD Year 2000 Management Plan, Version 2, December 1998.

Management Comments. The Director, Defense Security Service, concurred and stated that:

- DSS prepared draft system contingency plans for seven mission-essential systems and has scheduled workshops to prepare system contingency plans for its remaining eight mission-essential systems. Also, DSS drafted a separate system contingency plan for its enterprise database.

- DSS prepared a template that each DSS site will use to prepare its operational contingency plan. Each DSS site will complete and forward its operational contingency plan through its chain and to the DSS Year 2000 management team and senior management for final review.

- Management plans to finalize DSS system contingency and site operational contingency plans by September 30, 1999.

B. Defense Security Service Year 2000 Test-Related Issues

The DSS test plan did not have sufficient detail to adequately test 15[4] mission-essential systems for year 2000 compliance, and the test milestone dates for testing mission-essential systems and end-to-end testing were not realistic. Also, DSS did not prepare an end-to-end test plan to make an operational readiness assessment of its personnel security investigative and industrial security programs.

The DSS test plan was not sufficient because it did not require documentation of test results. DSS did not include the Student Information and Registration Network 01 in its test plan. The test milestone dates were unrealistic because DSS did not do the following:

- include testing of one mission-essential system,
- allocate sufficient time to retest or test mission-essential systems for year 2000 compliance, and
- allocate sufficient time to build a test bed to test mission-essential systems that have interdependencies.

DSS did not prepare an end-to-end test plan because DSS did not follow guidance in the DoD Year 2000 Plan.

As a result, there remains a risk that DSS mission-essential systems are susceptible to year 2000 related failures. Such failures could result in DSS not effectively accomplishing its mission.

Requirement for Test Plans

The DoD Year 2000 Plan requires DoD Components to prepare system test plans during the awareness phase and to modify the plans continuously during the evaluation of their systems. The DoD Year 2000 Plan states that, at a minimum, a test plan should show starting and ending dates for each phase, the major steps required to convert and test codes, and the identification of necessary infrastructure and resources required to accomplish those tasks. In addition, a test plan should be designed to provide assurance that mission operations would not be adversely affected in the year 2000 and beyond. Another requirement in the DoD Year 2000 Plan is that DoD Components complete testing of individual systems before demonstrating the year 2000 readiness of systems in an integrated, operational environment. The DoD Year 2000 Plan also requires that Principal Staff Assistants or designated Test

[4]Appendix B numbers 1 through 15.

Directors certify that end-to-end test plans include assessments of functional risk, effects of the year 2000 on continuity-of-business operations, and associated contingency plans. The DoD Year 2000 Plan states that Principal Staff Assistants are responsible for verifying that all functions under their purview would be unaffected by year 2000 issues.

Test Plan and Test Results

DSS Test Plan. The DSS test plan did not have sufficient detail to adequately test 15 mission-essential systems for year 2000 compliance. The test plan was a single document for all mission-essential systems located at the DSS Operations Center-Baltimore, Linthicum, Maryland. The test plan was incomplete because it did not include the Student Information and Registration Network 01 within the DSS Training Office.

The test plan was insufficient because it did not designate tests that were required for each system and did not show critical and other test dates required for year 2000 compliance. Also, the test plan did not identify contingent or backup capabilities for each system. After the audit team addressed deficiencies in the test plan and test schedule, DSS year 2000 management personnel provided a revised addendum to the test plan. The addendum described the process that DSS would use to retest eight systems that were previously tested but that lacked required documentation of test results and certification.

Documentation of Test Results. The DSS test plan was insufficient because it did not require documentation of test results. The DoD Year 2000 Plan provides a checklist in its Appendix G that system managers can use to certify year 2000 compliance of system tests and to record test results. Although DSS personnel used the DoD checklist to perform tests on mission-essential systems, they did not document test results and were unable to provide formal certifications for systems tested. In contrast, DSS personnel provided documentation for testing of personal and laptop computers, servers, and the FINCEN-Treasury System.

Although DSS year 2000 management personnel documented the test results for the FINCEN-Treasury System, the actual tests performed did not meet the requirements of the DoD Year 2000 Plan. The DSS year 2000 management personnel tested the system for the following dates: February 2 and 28, 2000; March 1, 2000; and February 2, 2002. The audit team informed a representative of the DSS year 2000 management team that the test results for the FINCEN-Treasury System did not include critical and other test dates required in the DoD Year 2000 Plan. Based on our discussions with a member of the DSS year 2000 management team, the DSS year 2000 management personnel decided to schedule the FINCEN-Treasury System for retesting. Later, the DSS year 2000 management personnel provided an addendum that revised the DSS test plan and test schedule that includes the FINCEN-Treasury System and the other seven systems requiring retesting. DSS needs to revise the test plan for the remaining seven systems that require testing.

DSS Test Schedule

The initial DSS test schedule provided did not show sufficient detail to track critical test events, did not include all 15 mission-essential systems to be tested, and did not allot days to build a test bed for end-to-end testing. DSS developed a three-phase test schedule. Phase I established the completion dates for retesting eight[5] mission-essential systems. Of the eight systems DSS planned to retest, DSS could not provide documentation and certifications for seven systems; and the test results of the remaining system did not meet the requirements of the DoD Year 2000 Plan. On March 24, 1999, after our discussions with DSS year 2000 management personnel regarding deficiencies in the test schedule, DSS provided a revised test schedule for the eight systems that require retesting. The revised test schedule showed the specific tests that DSS planned to conduct for the eight systems and revised dates. Although there was slippage from that schedule, as of early June 1999 the testing was reported to be nearly complete.

However, DSS did not provide a revised Phase II test schedule for seven mission-essential systems. Phase II testing was scheduled to begin March 5, 1999, and conclude August 3, 1999. Based on our review of the test schedule and other information, we concluded that DSS probably would not complete Phase II testing by August 3, 1999. Of the seven systems (see Appendix B) that DSS had to test, one system had to be replaced, one system was still being assessed for year 2000 compliance, and five systems were still in renovation. The contract to identify a replacement system for the Student Information and Registration Network 01 was awarded March 12, 1999, and DSS scheduled implementation of the new system by July 1, 1999. The Files Automation and Scanning Subsystem (FASS) contractor was still assessing the FASS for year 2000 compliance. Furthermore, DSS could not fully assess FASS for year 2000 compliance until a test bed was built to conduct end-to-end testing. Following our discussions with DSS year 2000 management personnel regarding the milestone dates for completing Phase II testing, DSS decided to complete Phase I retesting before starting Phase II testing. Therefore, DSS needs to revise its test schedule to reflect new milestone dates for Phase II testing.

DSS also needs to revise its test schedule to reflect new milestone dates for end-to-end testing. In its initial test schedule, DSS allotted 16 days, scheduled to begin July 13, 1999, and conclude July 30, 1999, for end-to-end testing. Based on information reviewed for end-to-end testing, we concluded that DSS probably would not complete end-to-end testing by July 30, 1999. The initial test schedule did not include time to build a test bed that was needed to test FASS and four other mission-essential systems that have interdependencies. DSS year 2000 management personnel contended that end-to-end testing could be completed within the allotted days because they would use test data rather

[5] The DSS test schedule initially showed seven systems requiring retesting. However, after reviewing the test results for the FINCEN-Treasury System, we determined that date tests were not sufficient to ensure the system's compliance in the year 2000 and beyond. Therefore, DSS year 2000 management personnel decided to retest the system.

than downloading system data to the test bed components. Also, they planned to use contractor personnel to build the test bed, which would make better use of available resources. Because of the revised milestones for Phase I testing and the decision not to start Phase II testing until Phase I is completed, DSS needs to revise its test schedule to reflect new milestone dates for end-to-end testing.

End-to-End Testing

DSS did not prepare an end-to-end test plan to test the integration and operational readiness of mission-essential systems used to process data to support its personnel security investigative and industrial security programs. An end-to-end test plan should specify the integrated systems to be tested; describe the layout of the test bed; specify the tests to be performed, results expected, resolution of discrepancies, and exit criteria; and specify the type of certification to be used, such as self or third-party certification. The DoD Year 2000 Plan requires DoD Components to conduct end-to-end testing to ensure the complete flow of data through a set of interconnected systems that perform a core business process, function, or mission. Although they do not have direct connectivity to each other, 14[6] of the 15 DSS mission-essential systems have internal dependencies through the shared Oracle database used to support the personnel security investigative and industrial security programs. Of the 14 systems, 4 systems[7] have external interface connectivity to other DoD and Federal organizations. Therefore, end-to-end testing of the 14 systems is extremely important to ensure the proper flow of data into and out of the systems and organizations.

End-to-End Test Plan. Because of the importance of end-to-end testing, the DoD Year 2000 Plan requires Principal Staff Assistants or designated Test Directors to provide functional end-to-end test plans to the Deputy Secretary of Defense. The Principal Staff Assistants must certify that end-to-end test plans include assessments of functional risks, effects of the year 2000 on continuity-of-business operations, and associated contingency plans. To fulfill the requirement, the Principal Staff Assistants must receive end-to-end test plans from their components. DSS did not provide an end-to-end test plan to the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), its Principal Staff Assistant. To ensure the validity of DSS end-to-end testing, the Director, DSS, should prepare and provide an end-to-end test plan to the Principal Staff Assistant.

Interdependent Systems. Because of the interdependencies, DSS could not perform end-to-end testing for the Case Control Management System, the Disclosure Accounting System, the File Control Management System, and the DCII Disclosure Accounting System until FASS is year 2000 compliant.

[6]Appendix B numbers 1 through 15, except number 10, Reject Tracking System.

[7] The four systems are the Case Control Management System, Defense Clearance and Investigations Index Disclosure Accounting System, Automated File Requests System, and FINCEN-Treasury System.

Although FASS was operational, DSS could not perform FASS year 2000 compliance and end-to-end testing before building a test bed.

Files Automation and Scanning Subsystem. FASS provides a vehicle to convert the following:

- prior investigative files from microfiche to image,
- paper received in the process of conducting investigations from paper to image, and
- hard copy of information on personnel security questionnaire forms into electronic data.

Through the use of various electronic media, FASS distributes the results of completed investigations to security clearance adjudicators. FASS also services requests of DSS files from authorized requestors and requests of DSS files in support of the Freedom of Information Act. FASS manages the storage and retrieval of all images associated with investigative files. An extensive internal interface exists between the Case Control Management System and FASS in the form of stored Oracle database procedures.

Since September 2, 1997, DSS stored all closed cases as images rather than microfiche. On October 29, 1998, all other functions of FASS became operational along with the Automated File Requests System, the Case Control Management System, the DCII, the DCII Disclosure Accounting System, the Disclosure Accounting System, the Electronic Personnel Security Questionnaire, and the User Community Management System.

Year 2000 Compliance of FASS. DSS was not assured of the year 2000 compliance of FASS because year 2000 contract clauses were not included in the DSS statement of work for FASS or in the FASS contract prepared by the contracting activity.

Compliance Requirement in Contracts. The Office of Management and Budget "Year 2000 Federal Acquisition Guidance," January 9, 1997, states that year 2000 procurement guidance developed for inclusion in the Federal Acquisition Regulations was issued in Federal Acquisition Circular 90-45. The guidance provided agencies with year 2000 information that would be helpful when awarding new information technology contracts or modifying older ones. The guidance, which was effective January 1, 1997, was an interim rule to ensure that Federal agencies only acquired year 2000 compliant products and systems. On October 21, 1997, the interim rule was finalized. The final rule states that solicitations and contracts should require year 2000 compliant

technology or should require that noncompliant information technology systems be upgraded and made compliant in a timely manner. Agencies are expected to test upgraded and new systems for year 2000 compliance.

FASS Contract. The FASS development was contracted on a blanket purchase agreement through the Department of Veterans Affairs with Science Applications International Corporation. The blanket purchase agreement became effective March 28, 1997. Neither the DSS statement of work nor the Department of Veterans Affairs basic contract required year 2000 compliance.

Assessment of FASS. Before the issuance of the draft to this report, Science Applications International Corporation was assessing FASS to determine year 2000 compliance. In its comments to the draft report, DSS management stated that the contractor had completed its assessment of FASS and that DSS was reviewing the results of the contractor's assessment.

Although DSS year 2000 management personnel knew about the need for end-to-end testing, they did not schedule the testing because of the unknown status and time line of FASS and the need for additional funding for a test bed. DSS received $50,000 in year 2000 supplemental funding. As a result of that funding, DSS was in the process of contracting to have the FASS test bed built and to have the proposed contractor assist in conducting FASS year 2000 compliance testing. This testing will tie into the DSS enterprise end-to-end testing for mission-essential application systems. The DSS goal is to have end-to-end test planning completed by June 25, 1999.

Conclusion

To improve the likelihood that it will be able to perform its mission in the year 2000 and beyond, DSS must prepare comprehensive test plans and conduct effective system tests and end-to-end testing.

Testing is one of the final and most challenging phases in an organization's year 2000 planning and management strategy. To minimize year 2000 related system failures, an organization must prepare detailed written test plans and conduct both system tests and end-to-end tests of integrated systems. System tests are the lowest level of tests designed to prove individual system readiness. That level of testing identifies functions and missions, associates those functions and missions with automated systems, and verifies that the functions and missions can be conducted in the year 2000 environment. Upon completion of individual system tests, end-to-end testing should be conducted to demonstrate the year 2000 readiness of systems in an integrated, operational environment.

The implementation of the following recommendations should improve the effectiveness of system and end-to-end testing and reduce the likelihood of mission disruptions from year 2000 system-related failures at DSS.

Recommendation and Management Comments

B. We recommend that the Director, Defense Security Service:

1. Revise the Defense Security Service test plan to address year-2000 compliance testing required for each mission-essential system. The DoD Year 2000 Management Plan, Version 2.0, December 1998, should be used as the framework to develop the revised test plan.

2. Revise the Defense Security Service test schedule to reflect new milestone dates for Phase II and end-to-end testing.

3. Complete the retesting of previously tested systems that lacked formal documentation and certification and test the remaining Defense Security Service mission-essential systems; document test results for all systems; and certify all systems as year 2000 compliant upon successful completion of the tests.

4. Prepare an end-to-end test plan that would address the integrated systems to be tested, layout of the test bed, the tests to be performed, results expected, resolution of discrepancies, exit criteria, and certification to be used.

5. Provide the end-to-end test plan to the Year 2000 Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) for review of technical adequacy.

Management Comments. The Director, Defense Security Service concurred with the recommendations. DSS has used the DoD Year 2000 Management Plan as a framework to complete an initial review of its test plan. DSS plans to revise its test schedule to reflect new milestone dates for system and end-to-end testing. DSS plans to retest previously tested systems to formally document results and test all remaining mission-essential systems. DSS will provide an end-to-end test plan to the Year 2000 Office of the Assistant Secretary of Defense when it is available. The DSS goal is to have the test schedule revised by June 4, 1999, and the end-to-end test plan completed by June 25, 1999.

Appendix A. Audit Process

This report is one in a series that the Inspector General, DoD, issued in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor efforts to address the year 2000 computing challenge. For a listing of audit projects addressing this issue, see the year 2000 webpage on Inspector General Internet at http://www.ignet.gov.

Scope

Work Performed. We reviewed actions taken by DSS to resolve year 2000 date-processing issues for 24 mission-essential systems. In addition, we reviewed system implementation schedules, test plans, test results, and contingency plans to address year 2000 related system failures that could impact the ability of DSS to perform its mission. We also reviewed briefing charts and reports provided to DoD on systems identified and their status.

DoD-Wide Corporate-Level Government Performance and Results Act Goals. In response to the Government Performance and Results Act, the Department of Defense established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting those objectives. This report pertains to achievement of the following objectives and goals.

- **Objective:** Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. **(DoD-3)**

- **Objective:** Fundamentally reengineer DoD and achieve a 21st century infrastructure. **Goal:** Reduce costs while maintaining required military capabilities across all DoD mission areas. **(DoD-6)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals in the Information Technology Management Functional Area:

- **Objective:** Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM 1.2)**

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate DoD information infrastructure. **(ITM 2.2)**

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Upgrade the technology base. **(ITM2.3)**

- **Objective:** Ensure that vital information on DoD resources is secure and protected. **Goal:** Assess information assurance posture of DoD operational systems. **(ITM 4.4)**

General Accounting Office High-Risk Area. The General Accounting Office identified several high-risk areas in the DoD. This report provides coverage of the Defense Information Management and Technology high-risk areas.

Methodology

To evaluate DSS efforts to achieve year 2000 compliance, we reviewed 24 DSS mission-essential systems. We also reviewed the DSS mission to identify each organizational unit and its associated information technology systems. For each system reviewed, we did the following:

- determined whether DSS identified, and properly classified all systems essential to accomplishing its mission;
- determined whether DSS had scheduled the full implementation of year 2000 compliant systems;
- reviewed systems reported in the DoD database as of March 10, 1999, and systems reported to the Office of Management and Budget;
- reviewed the adequacy of contingency plans, test plans, and test results for each system;
- determined whether DSS had prepared operational contingency plans; and
- determined whether DSS identified year 2000 funding shortfalls and requested additional funds or made necessary provisions to eliminate year 2000 funding shortfalls.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Audit Period, Standards, and Locations. We conducted this economy and efficiency audit from January through April 1999, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the year 2000 issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance.

Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to year 2000 issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil.

Appendix B. Defense Security Service Mission-Essential Systems

	System	Identifier	Compliance Completion Date	Contingency Plan	Cert.[1] Level
1	Case Control Management System	CCMS	Dec. 23, 1998	No	3a[2]
2	Defense Clearance and Investigations Index	DCII02	Dec. 23, 1998	No	3a
3	Automated File Requests	AFR01	Dec. 23, 1998	No	3a
4	DCII Disclosure Accounting System	DDAS01	Dec. 23, 1998	No	3a
5	Disclosure Accounting System	DAS	Dec. 23, 1998	No	3a
6	Electronic Personnel Security Questionnaire	EPSQ01	Dec. 23, 1998	No	3a
7	User Community Management System	UCMS01	Dec. 23, 1998	No	3a
8	FINCEN Treasury (CCMS Treasury Fincen)	Fincen02	Mar. 12, 1999	No	3a
9	File Control Management System	FCMS	Mar. 19, 1999	No	4[3]
10	Reject Tracking System	RTS01	Mar. 19, 1999	No	4
11	Files Automation and Scanning Subsystem[4]	FASS	July 1, 1999	No	4
12	Industrial Security System	ISS-01	July 1, 1999	No	4
13	Automated Credit Manager (CCMS Credit)	ACM01	Sept. 30, 1999	No	4
14	Field Agent Manager	FAM	Sept. 30, 1999	No	4
15	Student Information and Registration Network	SIRN02	Sept. 30, 1999	No	4
16	Field Information Management System	FIMS01	To Be Retired Sept. 30, 1999	No	4
17	Student Information and Registration Network	SIRN01	To Be Retired Sept. 30, 1999	No	4
18	Automated Credit Reporting System	ACRS01	Retired	N/A	0[5]
19	Automated Scoping Guide	ASGS01	Retired	N/A	0
20	Defense Clearance and Investigations Index	DCII01	Retired	N/A	0
21	Defense Integrated Management System	DIMS01	Retired	N/A	0
22	Joint Adjudication and Clearance System	JACS01	Retired	N/A	0
23	MEAD	MEAD01	Retired	N/A	0
24	Treasury Finance Center	Fincen01	Retired	N/A	0

[1]Certification.
[2]3a – Self-certification with full use of 4-digit century date fields.
[3]4 – Not certified or system requires additional work.
[4]This system is in the assessment phase.
[5]0 - System retired or replaced.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Acquisition and Technology)
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense for (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence, Surveillance, Reconnaissance, and Space Systems)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
    Principal Director for Year 2000
Assistant Secretary of Defense (Public Affairs)

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Chief Information Officer, Department of the Army
Inspector General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Auditor General, Department of the Navy
Chief Information Officer, Department of the Navy
Inspector General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force
Chief Information Officer, Department of the Air Force
Inspector General, Department of the Air Force

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Director, Defense Intelligence Agency
  Inspector General, Defense Intelligence Agency
Director, Defense Security Service
  Inspector General, Defense Security Service
  Deputy Director for Service, Defense Security Service
  Director, DoD Polygraph Institute
  Director, Security Research Center
Defense System Management College
Director, Washington Headquarters Services

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs
General Accounting Office
  National Security and International Affairs Division
    Technical Information Center
  Director, Defense Information and Financial Management Systems, Accounting and Information Management Division, General Accounting Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Special Committee on the Year 2000 Technology Problem
Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Committee on Government Reform and Oversight
House Committee on Armed Services

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd.)

House Subcommittee on Defense, Committee on Appropriations
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs and International Affairs, Committee on Government Reform and Oversight
House Subcommittee on Technology, Committee on Science

Defense Security Service Comments

DEFENSE SECURITY SERVICE
1340 BRADDOCK PLACE
ALEXANDRIA, VA 22314-1651

MAY 1 9 1999

MEMORANDUM FOR DIRECTOR, ACQUISITION MANAGEMENT DIRECTORATE (DoDIG)

SUBJECT Defense Security Service's (DSS) Response to Audit Report on Year 2000 Conversion Within the Defense Security Service (Project No 9AD-0084)

We have reviewed the audit report dated April 20, 1999, and have provided comments in an attachment to this memorandum We concur with all of the recommendations and have provided comments describing actions taken or planned and completion dates where appropriate DSS has made significant progress in many areas of its Year 2000 compliance with the goal of assuring uninterrupted operational capability Actions have been initialized in all areas where you have cited issues or concerns A formal briefing on the results of the audit is requested if the final report is revised and/or differs from the draft

We appreciate the time and efforts of your audit staff Should you have any questions or require further clarification on any issues, you may contact Ms Charlene S Jensen of my staff at (410) 865-2631 or email at charlene jensen@mail.dss mil

for Sheila D Dryden
STEVEN T SCHANZER
Director

Attachment

Final Report Reference

Reference Audit Report on Year 2000 Conversion Within the Defense Security Service (Project No 9AD-0084), dated April 20, 1999.

Revised Page 5

1 Page ii, Executive Summary (ES), Summary of Recommendations: DSS concurs with the Summary of Recommendations All Y2K planning, preparation, testing, etc. will be in accordance with the DoD Year 2000 Management Plan DSS is preparing system contingency plans for each mission-essential system and operational contingency plans for each site location Draft contingency plans have been prepared and are presently being reviewed for the following seven systems Electronic Personnel Security Questionnaire (EPSQ), FINCEN, Industrial Security System (ISS), User Community Management System (UCMS), Defense Clearance and Investigations Index (DCII), Training, and Credit Workshops are being scheduled to prepare system contingency plans for the following eight systems: Files Automation and Scanning Subsystem (FASS), Reject Tracking System (RTS), Case Control Management System (CCMS), Authorized File Request (AFR), File Control Management System (FCMS), Disclosure Accounting System (DAS), DCII Disclosure Accounting System (DDAS), and Field Agent Manager (FAM) A separate system contingency plan for the enterprise database has been drafted and is in review The goal for finalizing DSS system contingency plans is September 30.

Revised Page 6

2 Page ii, ES, Summary of Recommendations: A template has been prepared to be used for operational contingency plans for each DSS site. This plan is being staffed and will be reviewed onsite at an Operating Location (OL) Headquarters. Each DSS site will complete and forward their operational contingency plans through their chain, to the DSS Year 2000 management team and senior management for final review The DSS goal for finalizing operational contingency plans is September 30.

3 Page ii, ES, Summary of Recommendations: DSS has used the DoD Year 2000 Management Plan as a framework to complete an initial revision of its test plan. DSS plans to revise its test schedule to reflect new milestone dates for system and end-to-end testing DSS plans to retest previously tested systems to formally document results and test all remaining mission-essential systems. DSS will provide an end-to-end test plan to the Year 2000 Office of the Assistant Secretary of Defense when it is available

Revised Page 6

4 Page 1, Background, Defense Security Service Missions: As of May 17, DSS has 1150 Special Agents and 208 Industrial Security Representatives in remote locations

5 Page 6, Contingency Planning Section, Operational Missions: The Security Research Center (SRC) has completed a thorough Y2K compliance review of all information technology (IT) components. All IT components will be Y2K compliant by June 30, 1999 SRC's operational contingency plan will also be completed by June 30, 1999

The Y2K compliance review at the SRC addressed the following IT components: computer systems, telecommunications equipment and services, interface components,

Final Report Reference

Revised Page 6 & 7

office equipment, and building alarms The Y2K compliance status for each is summarized below.

a Computer systems: All SRC operational hardware is Y2K compliant Of 120 software applications currently in use, 98 (82%) are fully compliant and 22 (18%) are not None of these 22 are essential to SRC operations These 22 software applications, however, are of value to SRC researchers. Of the 22, 16 are currently being patched or upgraded for Y2K compliance. For the remaining 6 applications, policy concerning future use has been established (e g., not to use non-compliant components of the applications, archive applications for documentary purposes) All applications in use at SRC will be fully compliant by June 30, 1999.

b SRC's telecommunications equipment and services are Y2K compliant.

c Interface components. SRC will be fully compliant in this area by May 30, 1999, when a new interface component is installed

d. All SRC office equipment is Y2K compliant

e SRC's building alarm system is Y2K compliant

6 Page 8, Contingency Planning, Recommendations As mentioned and expanded on in item 1 above, DSS concurs with a) the recommendations to prepare system contingency plans, and b) operational contingency plans.

7 Page 14, Defense Security Service Year 2000 Test-Related Issues Section, Assessment of FASS· Science Applications International Corporation (SAIC) has completed their analysis of the Files Automation and Scanning Subsystem (FASS) which consists of Commercial Off-the-Shelf (COTS) hardware and software, and SAIC-developed software. SAIC used the Utility 2000 (U2K) tool, a source code checker, to analyze SAIC-developed software. All SAIC developed software was run through the U2K process twice The U2K tool produced a threat assessment that provided potential Year 2000 issues, which need to be further examined by DSS.

SAIC provided the analysis for each FASS COTS hardware and software product by listing the product with a statement regarding compliance. If not compliant, SAIC has provided a statement of each action to be taken (e g , replace software, upgrade hardware, etc) if known DSS is presently reviewing the results of this analysis

DSS is in the process of contracting the $50,000 received in Year 2000 supplemental funding The proposed contractor will provide a cost estimate to build a FASS test bed and assist in conducting FASS Year 2000 compliance testing. This will tie into the DSS enterprise end-to-end testing for mission-critical application systems

8 Page 15, Defense Security Service Year 2000 Test-Related Issues Section, Recommendation

a DSS concurs that the test plan needs to be revised to address Year 2000 compliance testing that is required for each mission-essential system The DoD Year 2000 Management Plan is being used in developing this plan The goal is to have the test plan revised by June 4, 1999

b. DSS will revise the test schedule to reflect new milestone dates for Phase II and end-to-end testing This schedule will be based upon planned availability of renovated systems and will be modified where necessary when planned availability differs from the actual delivery dates of the renovated systems The enterprise end-to-end testing is contingent upon the FASS test bed being built The contingency is to test without FASS

c DSS concurs with the recommendations regarding testing, documentation and certification of the test results DSS will retest all previously tested systems that lacked formal documentation and certification DSS will test all remaining mission-essential systems, formally document test results, and certify compliance upon completion of the testing

d DSS concurs and they will prepare an end-to-end test plan as detailed in the recommendation The goal is to have the end-to-end test plan completed by June 25

e DSS concurs and they will provide the end-to-end test plan when completed to the Year 2000 Office of the Assistant Secretary of Defense for review of technical adequacy

Audit Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Thomas F. Gimble
Robert K. West
Yvonne M. Speight
Lois A. Therrien
Ellen Neff
Stanley Arceneaux